WHAT IS CLAIMED IS:

1. A method for creating a secure sub-network on a public network, the public network including a set of devices, the secure sub-network to include a subset of devices from among the set of devices, said method comprising the steps of:

providing an access card having a first private key comprised thereon;

scanning the access card to determine the first private key, by the subset of devices;

determining a master device from among the subset of devices;

selecting a second private key and computing a public key based on the second private key, by the master device, the second private key only known to the master device;

sending the public key to the set of devices, by the master device; and

computing a shared encryption key, and requesting an encryption of any subsequent messages between any of the devices comprising the subset of devices using the shared encryption key.

2. The method according to claim 1, further comprising the step of programming the subset of devices with at least two parameters, wherein said steps of computing the public key and the shared encryption key are based on the at least two parameters.

3. The method according to claim 1, further comprising the step of requesting a MAC ID from each of the subset of devices, by the master device.

4. The method according to claim 3, further comprising the step of sending a message from at least one device of the

subset of devices to at least one other device of the subset of devices, using the MAC ID of the at least other device and the encryption key Z.

5. The method according to claim 1, further comprising the step of imposing a time restriction on the access card, wherein the access card is valid only for a predefined time period.

6. The method according to claim 5, further comprising the step of renewing a validity of the access card subsequent to the predefined time period.

7. The method according to claim 6, wherein said renewing step comprises the step of imposing a fee to renew the validity of the access card.

8. A method for creating a secure sub-network on a public network, the public network including a set of devices, the secure sub-network to include a subset of devices from among the set of devices, the subset of devices being programmed with two numbers g and n, said method comprising the steps of:

providing an access card having a secure number x comprised thereon;

scanning the access card to determine the secure number x, by the subset of devices;

determining a master device from among the subset of devices;

selecting a number y and computing $Y = g^y \bmod n$, by the master device, the number y only known to the master device;

sending Y to the set of devices, by the master device; and

requesting an encryption of any subsequent messages between any of the devices comprising the subset of devices using an encryption key $Z = (g^Y)^X \bmod n$.

9. The method according to claim 1, further comprising the step of imposing a time restriction on the access card, wherein the access card is valid only for a predefined time period.

10. The method according to claim 9, further comprising the step of renewing a validity of the access card subsequent to the predefined time period.